UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,251	05/11/2001	Sarver Patel	18	7868

7590 04/05/2005

Docket Administrator (Room 3C-512)
Lucent Technologies Inc.,
600 Mountain Avenue
P.O. Box 636
Murray Hill, NJ 07974-0636

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/854,251	PATEL, SARVER	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. Applicant's arguments filed 10 November 2004 have been fully considered but they are not persuasive.

2. Referring to the rejection of claim 1, the Applicant contends and argues that the prior art Bellare et al. does not teach or suggest processing the message by alternative procedures, depending on the size of the message relative to an input block, nor provide a single iteration involving nested functions. The Examiner disagrees and asserts that Bellare et al. does teach alternative procedures of message authentication by incorporating NMAC and HMAC. The cryptographic strength of NMAC allows a message according to the size relative of the input block, providing a nested iterative hash function for each message. (See page 9, Section 4 and page 10, Section 4.2) Bellare also teah another message authentication procedure known as HMAC. As shown on page 13, Sections 5 and 5.1, a single iteration using a nested function is performed using the HMAC function. HMAC and NMAC performing together will provide a more secure process for message authentication. (See page 14, Section 5.2)

3. Referring to the rejection of claim 7, the Applicant contends and argues that the prior art Bellare et al. does not teach or suggest hashing only one portion of the message, providing both portions of the message as inputs to a hash function, much less a keyed hash function. The Examiner disagrees and asserts that Bellare et al. does teach hashing one portion of a message by using keyed hash functions. The hashing function (F) is applied to the first portion of a message (data x) using the keyed IV. The

keyed IV performs keyed hash functions for each individual function within the first portion by using its corresponding key. (See page 8, Section 3)

Bellare also teach the first and second portions of a message used as inputs to a hash function by using secretly keyed hash functions. This method prevents an attacker from determining the key which was used to hash the message. (See page 9, Section 3.1)

4. Therefore, the rejection of claims 1-18 are maintained in view of the reasons above and in view of the reasons below.

DETAILED ACTION

1. Claims 1-18 are pending.

2. The Information Disclosure Statements respectfully submitted on 14 May 2001, 8 July 2002, and 26 January 2004 have been considered by the Examiner.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al. (Keying Hash Function for Message Authentication).

Referring to the rejection of claims 1,8, and 14, Bellare et al. discloses a method of processing a message for authentication comprising: performing a single iteration of a compression function using a key and the message as inputs when the message fits

within an input block of the compression function and using a hash function nested within a keyed hash function to process the message when the message does not fit within an input block of the compression function (See page 3, Section 1.3, page 6, Section 2, page 7, and page 10, Section 4)

As per claims 2,7,15, and 16, Bellare et al. discloses a method comprising the steps of: providing a first portion and a second portion of the message, performing a hash function using the first portion as an input to achieve a result, and performing a keyed hash function using the second portion and the result as inputs (See pages 7-9)

As per claims 3 and 10, Bellare et al. discloses the claimed limitation wherein the hash function is an iterated hash function F and the keyed hash function is a keyed compression function F (See pages 7-9)

As per claims 4 and 11, Bellare et al. discloses the claimed limitation wherein the hash function is an iterated hash function F and the keyed hash function is an iterated hash function F (See pages 7-9)

As per claims 5 and 12, Bellare et al. discloses a method comprising the steps of: using a result from the compression function to produce a message authentication code and sending the message authentication code in association with the message for authenticating the message using the message authentication code (See page 16)

As per claims 6 and 13, Bellare et al. discloses a method comprising the steps of: using a result from the compression function to produce a message authentication code and comparing the message authentication code to a received message authentication code

received with the message, whereby the message is authentic if the message authentication code and the received authentication code match (See page 3, Section 1.1)

As per claims 9,17, and 18, Bellare et al. discloses a method comprising the steps of: determining whether the message fits within an input block of a compression function and performing a single iteration of a compression function using a key and the message as inputs when the message fits within an input block of the compression function (See page 15, Section 6)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-

272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
March 24, 2005

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

CLAIMS:

1. A method of processing a message for authentication, said method comprising:

performing a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function; and

using a hash function nested within a keyed hash function to process said message when said message does not fit within an input block of said compression function.

2. The method of claim 1 wherein said step of using comprises the steps of:

providing a first portion and a second portion of said message;

performing a hash function using said first portion as an input to achieve a result; and

performing a keyed hash function using said second portion and said result as inputs.

3. The method of claim 2 wherein said hash function is an iterated hash function F and said keyed hash function is a keyed compression function f.

4. The method of claim 2 wherein said hash function is an iterated hash function F and said keyed hash function is an iterated hash function F.

5. The method of claim 1 further comprising the steps of:

using a result from said compression function to produce a message authentication code; and

sending said message authentication code in association with said message for authenticating said message using said message authentication code.

6. The method of claim 1 further comprises:

using a result from said compression function to produce a message authentication code; and

comparing said message authentication code to a received message authentication code received with said message, whereby said message is authentic if said message authentication code and said received authentication code match.

7. A method of processing a message for authentication, said method comprising:

providing a first portion and a second portion of said message;

performing a hash function using said first portion as an input to achieve a result; and

performing a keyed hash function using said second portion and said result as inputs.

8. The method of claim 7 comprising the step of:

determining whether said message fits within an input block of a compression function; and

performing said steps of providing, performing and performing when said message does not fit within an input block of said compression function.

9. The method of claim 7 comprising the step of:

determining whether said message fits within an input block of a compression function; and

performing a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function.

10. The method of claim 7 wherein said hash function is an iterated hash function F and said keyed hash function is a keyed compression function f.

11. The method of claim 7 wherein said hash function is an iterated hash function F and said keyed hash function is an iterated hash function F.

12. The method of claim 7 further comprising the steps of:

using a result from said keyed hash function to produce a message authentication code; and

sending said message authentication code in association with said message for authenticating said message using said message authentication code.

13. The method of claim 7 further comprises:

using a result from said keyed hash function to produce a message authentication code; and

comparing said message authentication code to a received message authentication code received with said message, whereby said message is authentic if said message authentication code and said received authentication code match.

14 A message authentication system comprising:

processing circuitry configured to perform a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function and to use a hash function nested within a keyed hash function to process said message when said message does not fit within an input block of said compression function.

15. The system of claim 14 wherein said processing circuitry configured to provide a first portion and a second portion of said message, perform a hash function using said first portion as an input to achieve a result, and perform a keyed hash function using said second portion and said result as inputs.

16. A message authentication system comprising:

processing circuitry configured to provide a first portion and a second portion of said message, perform a hash function using said first portion as an input to achieve a result, and perform a keyed hash function using said second portion and said result as inputs.

17. The system of claim 16 wherein said processing circuitry configured to determine whether said message fits within an input block of a compression function.

18. The system of claim 17 wherein said processing circuitry configured to perform a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function.